AMENDMENTS TO THE SPECIFICATION:

Please amend the specification as follows:

Please replace the paragraph beginning on page 7, line 3, with the following amended paragraph:

Well-known cryptographic techniques can be used to generate credentials 105. For example, as shown in Fig. 2, in some embodiments credential 105 is formed by applying a strong cryptographic hash algorithm (e.g., SHA-1) 202 to the application 200 (or to selected portions thereof) to yield hash or message digest 204. Message digest 204 (and, in some embodiments, identification information 207) is encrypted (206) using the certification service's (or credential authority's) private key 208 to yield credential or signature 210. One of ordinary skill in the art will recognize that a number of variations could be made to the process shown in Fig. 2. For example, in some embodiments, a checksum of all or part of the application could be used instead of, or in addition to, the hash or message digest 204. It will be appreciated that there are a variety of other techniques for generating a credential or certificate for an application, and that for purposes of practicing the present invention any suitable technique can be used. For example, use could be made of the techniques described in Menezes at pages 1-45 and 283-488, the '900 patent, commonly-assigned U.S. Patent No. 6,157,721, entitled "Systems and Methods Using Cryptography to Protect Secure Computing Environments," issued December 5, 2000 ("the '721 patent"), commonly-assigned U.S. Patent Application ~~No. 60/146,426,~~ No. 09/628,692, entitled "Systems and Methods for Using Cryptography to Protect Secure and Insecure Computing Environments," ~~filed July 29, 1999,~~ and commonly-assigned U.S. Patent Application No. [_____]

All reviewed - FP 3/8/05

All reviewed -PP 3/8/05

09/863,199, entitled "Trust Management Systems and Methods," filed May 21, 2001, each of which is hereby incorporated by reference in its entirety. In other embodiments, the use of a special certificate or credential (it should be noted that, in general, these two terms will be used interchangeably) could be dispensed with, and verification of the certification or authorization of an application, user, or content object could simply be inferred based on possession of a cryptographic key (e.g., a private or secret key) and/or other secret (or not so secret) information.

Please replace the paragraph beginning on page 13, line 11, with the following amended paragraph:

All reviewed -PP 3/8/05

It should be noted that the nesting properties described above are not limited to application programs and portable devices, but can also be applied to virtually any program, device, process, or entity. For example, in one embodiment multiple digital rights management systems can be chained in the manner described above. Such a process can be facilitated using the techniques described in commonly-assigned Patent Application No. [_____] 09/874,744, entitled "Systems and Methods for Governing Content Rendering, Protection, and Management Applications," filed June 4, 2001, which is hereby incorporated by reference in its entirety.